12TH ICCRTS

"Adapting C2 to the 21st Century"

Game Theoretic Solutions to Cyber Attack and Network Defense Problems

Assigned Track: Network and Networking (Track 2)
Assigned Paper Number: I-062

Dan Shen
Intelligent Automation, Inc
15400 Calhoun Drive, Suite 400
Rockville, MD 20855
Tel: (301)294-5235
Email: dshen@i-a-i.com

Genshe Chen (Principal point of contact)
Intelligent Automation, Inc.
15400 Calhoun Drive, Suite 400
Rockville, MD 20855
Tel: 301 294 5218 (direct)
Fax: 301 294 5201
Email: gchen@i-a-i.com

Jose B. Cruz, Jr.,
The Ohio State University
205 Dresses Laboratory, 2015 Neil Ave
Columbus, OH 43202
Ph: (614)292-1588
Email: cruz.22@osu.edu

Erik Blasch
AFRL/SNAA
Erik.Blasch@WPAFB.AF.MIL

Martin Kruger
The Office of Naval Research
Email: Martin_Kruger@onr.navy.mil

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2007		**00-00-2007 to 00-00-2007**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Game Theoretic Solutions to Cyber Attack and Network Defense Problems	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Intelligent Automation, Inc,15400 Calhoun Drive, Suite 400,Rockville,MD,20855**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
Twelfth International Command and Control Research and Technology Symposium (12th ICCRTS), 19-21 June 2007, Newport, RI

14. ABSTRACT
There are increasing needs for research in the area of cyber situational awareness. The protection and defense against cyber attacks to computer network is becoming inadequate as the hacker knowledge sophisticates and as the network and each computer system become more complex. Current methods for alert correlation to detect and identify network attacks rely on data mining approaches that use features or feature sets of network data to discover an attack. These approaches are useful for simple attacks but for complex or coordinated cyber intrusions, they have various issues such as false positive, limited scalability, limits on detecting new types of coordinated and sophisticated cyber attacks. Therefore, the cyberspace security requires next-generation network management and intrusion detection systems that combine both short-term sensor information and long-term knowledge databases to provide decision-support systems and cyberspace command and control. In this paper, we propose a game theoretic high level information fusion based decision and control framework to detect and predict the multistage stealthy cyber attacks. The main focus of this paper is to address the cyber network security problem from a system control and decision perspective and revise the Markov game model with the knowledge of the cyber attack domain.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**37**	

ABSTRACT

Game Theoretic Solutions to Cyber Attack and Network Defense Problems

There are increasing needs for research in the area of cyber situational awareness. The protection and defense against cyber attacks to computer network is becoming inadequate as the hacker knowledge sophisticates and as the network and each computer system become more complex. Current methods for alert correlation to detect and identify network attacks rely on data mining approaches that use features or feature sets of network data to discover an attack. These approaches are useful for simple attacks but for complex or coordinated cyber intrusions, they have various issues such as false positive, limited scalability, limits on detecting new types of coordinated and sophisticated cyber attacks.

Therefore, the cyberspace security requires next-generation network management and intrusion detection systems that combine both short-term sensor information and long-term knowledge databases to provide decision-support systems and cyberspace command and control. In this paper, we propose a game theoretic high level information fusion based decision and control framework to detect and predict the multistage stealthy cyber attacks. The main focus of this paper is to address the cyber network security problem from a system control and decision perspective and revise the Markov game model with the knowledge of the cyber attack domain.

Outline:

1. Introduction

There are increasing needs for research in the area of cyber situational awareness. The protection and defense against cyber attacks to computer network is becoming inadequate as the hacker knowledge sophisticates and as the network and each computer system become more complex. When evaluating the security of a network, it is rarely enough to consider the presence of isolated vulnerabilities. Large network typically contain multiple platforms and software packages and employ several modes of connectivity (also various types of intruders from internal (i.e. espionage) and external (i.e. terrorists) disgruntled people. Inevitably, such networks have security holes that escape notice of even the most diligent system administrators.

Cyber attacks in the past were generally one-dimensional, mainly in the form of denial of service (DoS) attacks, computer viruses or worms, or unauthorized intrusions (hacking). These attacks were mainly launched against websites, mail servers or client machines. This has fundamentally changed recently – cyber threats are undergoing a diversification that is resulting in multi-stage and multi-dimensional attacks that utilize and/or target a variety of attack tools and technologies. Most contemporary attacks, the latest generation of worms for instance, make use of a variety of different exploits, propagation methods, and payloads. Infected machines may be used to launch attacks against other targets or their data could be accessed or deleted. Even more worrisome, the trend is toward an intensification of this development, potentially resulting in the emergence of many more sophisticated cyber attacks.

Recent advances in applying data fusion techniques to cyber situation awareness are promising. Some pioneering works focused on high-level descriptions of these approaches are presented in [2] and [3]. Two cyber defense systems performing high level information fusion have been recently proposed by Prof. Moises Sudit and his co-workers. INformation Fusion Engine for Real-time Decision-making (INFERD) [4] and [5] efficiently correlates IDS alerts to identify individual attacks and provides situational measures of the network. Threat Assessment for Network Data and Information (TANDI) [6] fuses the information extracted from the individually identified attacks, to determine the entities threatened and to differentiate them by assigning threat scores.

In this paper, we introduce a highly innovative information fusion approach for detection and prediction of multistage stealthy cyber attacks. Our approach unifies INFERD/TANDI (successfully used in cyber network situation awareness) developed by UB team and Markov Game theoretical threat intent inference [1] developed by IAI team to provide a better solution. There are two main parts: data fusion module and dynamic/adaptive feature recognition module. Various log file entities Alters generated by Intrusion Detection Sensors (IDSs) or Intrusion Prevention Sensors (IPSs) are fed into the L1 data fusion components. The fused objects and related pedigree information are used by a feature/pattern recognition module to generate primitive prediction of intents of cyber attackers. High-level (L2 and L3) data fusion based on Markov game model, Hierarchical Entity Aggregation (HEA) are proposed to refine the primitive prediction generated in stage 1 and capture new unknown features. Markov (Stochastic) game

method is used to estimate the belief of each possible cyber attack graph. The captured unknown or new cyber attack patterns will be associated to related L1 results in dynamic learning block, which takes deception reasoning, trend/variation identification, and distribution model and calculation into account.

The rest of the paper is organized as follows. Section 2 describes our proposed framework. We will focus on our Markov model for cyber network defense. Section 3 discusses the simulation tool and simulation results. Finally, conclusions are drawn in Section 4.

2. Framework and Markov Game model for Cyber Network Defense

The framework of our proposed approach for cyber situation awareness and impact assessment is shown in Fig. 1. There are two fully coupled major parts: 1) Data fusion module (to refine primitive awareness and assessment; to identify new cyber attacks); and 2) Dynamic/adaptive feature recognition module (to generate primitive estimations; to learn new identified new or unknown cyber attacks).

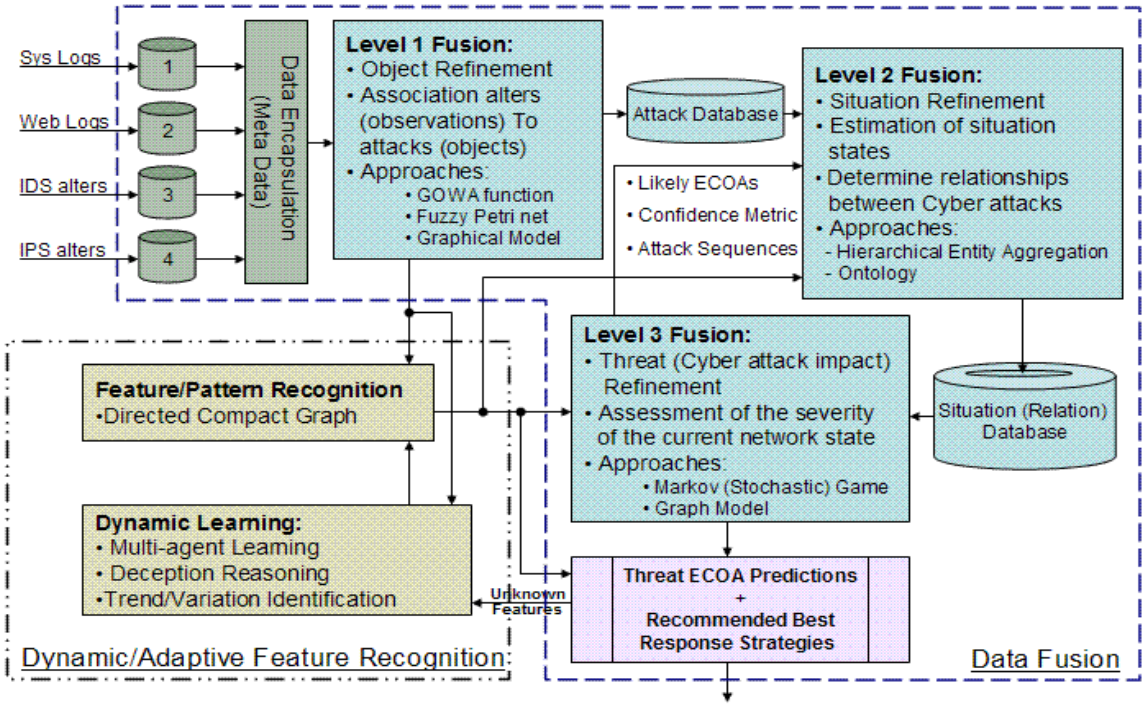


Fig. 1: A Game Theoretic Data Fusion Approach for Cyber Situation Awareness and Impact Assessment

Based on the input information of various logs and alters generated by Intrusion Detection Sensors (IDSs) or Intrusion Prevention Sensors (IPSs), level 1 fusion is carried out to generate objects and related pedigree information needed by a feature/pattern recognition module to generate primitive prediction of intents of cyber attackers. If the observed features are already associated with adversary intents, we can easily obtain them by pattern recognition. In some time-critical applications, the primitive prediction can be used before it is refined by relatively time-consuming high-level data fusion.

High-level (L2 and L3) data fusion based on Markov game model and Hierarchical Entity Aggregation (HEA) are proposed to refine the primitive prediction generated in stage 1 and capture new or unknown cyber attacks. Markov (Stochastic) game method is used to estimate the belief of each possible cyber attack graph. Game theory can capture the nature of cyber conflicts: the determination of the strategies of attacking force is tightly coupled to the determination of the strategies of the defense force and vice versa. Also it can deal with the uncertainty and incompleteness of the available information. We propose a graphical model to represent the structure and evolution of the above-mentioned Markov game model so that we can efficiently solve the graphical game problem.

The captured unknown or new cyber attack patterns will be associated to related L1 results in dynamic learning block, which takes deception reasoning, trend/variation identification, and distribution model and calculation into account. Our approach to deception detection is heavily based on the application of pattern recognition techniques to detect and diagnose what we call out-of-normal conditions in the cyber environment. The results of dynamic learning or refinement shall also be used to enhance L2 and L3 data fusion. This adaptive process may be considered as level 4 data fusion (process refinement, see JDL model).

Ontology and graphical model are exploited to design and represent the cyber attack related data and meta-information [7], such as recency, uncertainties, security, estimates, confidence, cost (availability and time) and pedigree information, so that the meta-information will be easily understood and used by data fusion and dynamic/adaptive learning modules.

In this paper, we will focus on the Markov game theoretic Level 3 data fusion solution in the overall architecture shown in Fig. 1. In general, a Markov (stochastic) game is specified by (i) a finite set of players N, (ii) a set of states S, (iii) for every player $i \in N$, a finite set of available actions D^i (we denote the overall action space $D = \times_{i \in N} D^i$), (iv) a transition rule $q: S \times D \to \Delta(S)$, (where $\Delta(S)$ is the space of all probability distributions over S), and (v) a payoff function $r: S \times D \to R^N$. For the cyber decision support and attacker intent inference problem, we obtain the following distributed discrete time Markov game (we revise the Markov game model [1] used for battle-space and focus on the cyber attack domain properties):

Players (Decision Makers) --- Cyber attackers, network defense system, and normal network users are players of this Markov game model. We denote cyber attackers as red team, network defense system (IDSs, Firewalls, Email-Filters, Encryption) as blue team, normal network user as white team. The cooperation within the same team is also modeled so that the coordinated cyber network attacks can be captured and predicted.

State Space --- All the possible states of involved network nodes consist of the state space. For example, the web-server (IP = 26.134.3.125) is controlled by attackers. To determine the optimal IDS deployment, we include the defense status for each network nodes in the state space. So for the i^{th} network node, there is a state vector $s^i(k)$ at time k.

$$s^i(k)=(f,p,a)^T \quad (1)$$

where f is the working status of the i^{th} network node, p is the protection status, T is the transpose operator, and a is the status of being attacked. "Normal" and "malfunction" are typical values of f with the meaning that the node is in the normal working status or malfunction (Recall that in battle space cases, the function status of any unit values can be "undestroyed", "damaged", or "destroyed"). p can be the defense unit/service (such as firewall, IDS and filter, with probability) assigned to the node and p = NULL means that the i^{th} node is unprotected. a is the status of being attacked. The type of attacks will be specified in Action Space.

Remark 1: It is not difficult to understand that the system states are determined by two factors: 1) previous states and 2) the current actions. So the whole system can be model by a first-order Markov decision process.

The overall system state at time k is

$$s_k=[s^1(k),s^2(k),\cdots,s^M(k)] \quad (2)$$

where M is the number of nodes in the involved cyber network.

Action Space --- At every time step, each player chooses targets with associated actions based on its local network information. For normal network users, the action types are http services, email services, ftp services, etc. The action-decision control of the i^{th} white player at time k is

$$u_w^i(k)=(t,v)^T \quad (3)$$

where vector t is the network node providing services and v is the service type requested. (We assume that the normal users know the server/service in advance). [Note: we use u for action decisions because action decisions typically are determined as utility functions with the higher payoff]

For red team (cyber network attackers), we consider the following types of *network-based attacks*:

- *Buffer overflow* (web attack): it occurs when a program does not check to make sure the data it is putting into a space will actually fit into that space. Vulnerability exists in Microsoft IIS 5.0 running on Windows 2000 that allows a remote intruder to run arbitrary codes on the victim machine, allowing them to gain complete administrative control of the machine. Apache HTTP Server version 1.3.19 could allow a remote attacker to send an HTTP request to cause the server to crash with unexpected behavior.
- *Semantic URL attack* (web attack): In semantic URL attack, a client manually adjusts the parameters of its request by maintaining the URL's syntax but altering its semantic meaning. This attack is primarily used against CGI driven websites. A similar attack involving web browser cookies is commonly referred to as cookie poisoning.
- *E-mail Bombing* (email attack): In Internet usage, an e-mail bomb is a form of net abuse consisting of sending huge volumes of e-mail to an address in an attempt to overflow the mailbox or overwhelm the server. The possible re-action is to

identify the source of the email bomb/spam and configure your router (or have your Network Service Provider configure the router) to prevent incoming packets from that address.

- *E-mail spam* (email attack): Spamming is the abuse of electronic messaging systems to send unsolicited, undesired bulk messages. Spammers often collect addresses of prospective recipients from use-net postings or from web pages, obtain them from databases, or simply guess them by using common names and domains. By popular definition, spam occurs without the permission of the recipients.
- *MALware attachment* (email attack): Malware is software designed to infiltrate or damage a computer system without the owner's informed consent. It is a blend of the words "malicious" and "software". Common MALware attacks are worms, viruses, trojan horses, etc.
- *Denial-of-service* (network attack): Denial-of-service (DoS) attack is an attempt to make a computer resource unavailable to its intended users. Typically the targets are high-profile web servers where the attack is aiming to cause the hosted web pages to be unavailable on the Internet. A distributed denial of service attack (DDoS) occurs when multiple compromised systems flood the bandwidth or resources of a targeted system, usually a web server(s). These systems are compromised by attackers using a variety of methods.

Remark 2: Some attacks may be multi-stage. For example, e-mail spam and MALware are used first to gain control of several temporal network nodes, which are usually not-well protected servers. Then DoS attack will be triggered to a specified and ultimate target. Our dynamic Markov game model can handle these attacks from a planning perspective. Our mixed Nash strategy pair is based on a fixed finite planning horizon. See Strategies for details.

For the blue team (network defense system), we consider the following *defense actions*:

- *IDS deployment*: we assume that there are limited IDSs. IDS deployment is similar to resource allocation (target selection) problems in traditional battle-space situations. We try to find an optimal deployment strategy to maximize the chance of detecting all possible cyber network intrusions.
- *Firewall configuration*: A firewall is an information technology (IT) security device which is configured to permit, deny or proxy data connections set and configured by the organization's security policy. Firewalls can either be hardware and/or software based.
- *Email-filter configuration*: Email filtering is the processing of e-mail to organize it according to specified criteria. Most often this refers to the automatic processing of incoming messages, but the term also applies to the intervention of human intelligence in addition to artificial intelligence, and to outgoing emails as well as those being received. Email filtering software inputs email and for its output, it might (a) pass the message through unchanged for delivery to the user's mailbox, (b) redirect the message for delivery elsewhere, or (c) throw the message away. Some e-mail filters are able to edit messages during processing.

- *Shut down or reset servers*.

Transition Rule --- The objective of the transition rule is to calculate the probability distribution over the state space $q(s_{k+1}|s_k,u_k^B,u_k^R,u_k^W)$, where s_k,s_{k+1} are system states at time *k* and *k+1* respectively, u_k^B,u_k^R,u_k^W are the overall decisions of the blue team (network defense system), the red team (cyber attackers) and the white team (normal network users), respectively, at time step *k*. How to decide the overall actions for each team are specified in Strategies.

For each network node (server or workstation), the state of time k+1 is determined by three things: 1) state at time *k*; 2) control strategies of the three teams; and 3) the attack/defense efficiency. If we compare part 3) to battle-space domain, the efficiency is the analogue of kill probability of weapons.

For example, if the state of node 1 at time *k* is ["normal", "NULL", "NULL"], one component of the red action is "email-bombing node 1", one component of blue action is "email-filter –configuration-no-block for node 1", and all white actions are not related to node 1, then the probability distribution of all possible next states of node 1 is: ["normal", "email-filter-configuration", "email-bombing"] with probability 0.4; ["slow response", "email-filter-configuration", "email-bombing"] with probability 0.3; and ["crashed", "email-filter-configuration", "email-bombing"] with probability 0.3. The actual probabilities depend on the efficiency of attacking and defending actions.

Payoff Functions --- In our proposed decentralized Markov game model, there are two levels of payoff functions for each team (red, blue, or white): lower (cooperative within each team) level and higher (non-cooperative between teams) level payoff functions. This hierarchical structure is important to model the coordinated cyber network attacks and specify optimal coordinated network defense strategies and IDS deployment.

The lower level payoff functions are used by each team (blue, red or white side) to determine the cooperative team actions for each team member based on the available local information. For the j^{th} unit of blue force, the payoff function at time *k* is defined as $\phi_j^B\left(\tilde{s}_j^B(k),u_j^B(k),W^B(k);k\right)$, where $\tilde{s}_j^B(k)\subseteq s_k$ is the local information obtained by the j^{th} blue member, $u_j^B(k)$ is the action taken by the blue team member at time *k*, and $W^B(k)$, the weights for all possible action-target couples of blue force, is announced to all blue team members and determined according to the top level payoff functions from a team-optimal perspective.

$$\phi_j^B\left(\tilde{s}_j^B(k),u_j^B(k),W^B(k);k\right) = U\left(\tilde{s}_j^B(k)\right) - w\left(W^B(k),u_j^B(k)\right)C\left(u_j^B(k)\right) \quad (4)$$

where, $U\left(\tilde{s}_j^B(k)\right)$ is the utility or payoff of the current local network state. Usually, it is a negative value if a network node is in malfunction status due to a cyber attack. The specific value depends on the value of the network node. The counterpart in the battle-space domain is the target value of each platform. Function $w\left(W^B(k),u_j^B(k)\right)$ will calculate the weight for any specified action decision for the j^{th} member of the blue team based on the received $W^B(k)$, which is determined on a team level and indicates the preference and

trend of team defense strategies. $C\left(u_j^B(k)\right)$ is the cost of action to be taken by the blue team member.

Similarly, we obtain the lower level payoff functions for the j^{th} member of red and white team,

$$\phi_j^R\left(\tilde{s}_j^R(k),u_j^R(k),W^R(k);k\right) = U\left(\tilde{s}_j^R(k)\right) - w\left(W^R(k),u_j^R(k)\right)C\left(u_j^R(k)\right) \tag{5}$$

$$\phi_j^W\left(\tilde{s}_j^W(k),u_j^W(k),W^W(k);k\right) = U\left(\tilde{s}_j^W(k)\right) - w\left(W^W(k),u_j^W(k)\right)C\left(u_j^W(k)\right) \tag{6}$$

Remark 3: It is well known that non-neutral civilians often play an active role in wars. That is, they are not just passively static but might purposefully take actions to help one side in a battle to minimize their losses or achieve some political purpose. Unfortunately, existing game theoretic models usually do not consider this situation, although collateral damage has been considered in a paper on a two-player game model by Cruz *et al* [8]. In this research, a three-player dynamic game model is formulated, in which two opposing forces and one normal player that might be either neutral or slightly biased [9]. In our current implementation, the white units only care about their possible losses. For an example, when a slower or malfunctioned network node is detected, normal network users will find a COA to keep themselves as far as possible from the node. In addition, there may be no cooperation between the white team members, so we can simply set $W^W(k)$ to 1.

Remark 4: In some instances of the use of game theory for military applications by others, it is almost always the case that zero-sum game theory is used. In zero-sum game theory, the players have opposite objectives. If one player maximizes an objective function, the other automatically minimizes it. This is equivalent to a player maximizing an objective function and the other player maximizing the negative of the same function. Since the sum of the objective functions is zero, the game is called a zero-sum game. But for the cyber network attack scenario, we propose a non-zero-sum game model for the following two reasons: 1) there are three players as mentioned in Remark 4; 2) even in the case without a white player, there are some cases the objective of attacking side and defense side are not opposite of each other. For example, the hackers may be deterred from any attacking actions by well-protected defense systems. In this case, payoffs of both sides decrease, which is conflicting the zero-sum assumption. So we model the cyber network attack and defense system as a non-zero-sum dynamic Markov game.

The top level payoff functions at time k are used to evaluate the overall performance of each team.

$$V^B(\tilde{s}^B(k),u_k^B;k) = \sum_{j=1}^{M^B} \phi_j^B\left(\tilde{s}_j^B(k),u_j^B(k),W^B(k);k\right) \tag{7}$$

$$V^R(\tilde{s}^R(k),u_k^R;k) = \sum_{j=1}^{M^R} \phi_j^R\left(\tilde{s}_j^R(k),u_j^R(k),W^R(k);k\right) \tag{8}$$

$$V^W(\tilde{s}^W(k),u_k^W;k)=\sum_{j=1}^{M^W}\phi_j^W\left(\tilde{s}_j^W(k),u_j^W(k),W^W(k);k\right) \quad (9)$$

In our approach, the lower lever payoffs are calculated distributedly by each team member and sent back to network administrator via communication networks.

Strategies --- In game theory, the Nash equilibrium (named after John Nash [10] who proposed it) is a kind of optimal collective strategy in a game involving two or more players, where no player has anything to gain by changing only his or her own strategy. If each player has chosen a strategy and no player can benefit by changing his or her strategy while the other players keep theirs unchanged, then the current set of strategy choices and the corresponding payoffs constitute a Nash equilibrium.

A mixed strategy is used in game theory to describe a strategy comprised of possible actions and an associated probability, which corresponds to how frequently the action is chosen. Mixed strategy Nash equilibria (NE) are equilibria where at least one player is playing a mixed strategy. It was proved by Nash that that every finite game has a Nash equilibria but not all has a pure strategy Nash equilibrium. While computing his mixed NE strategy, each player pays attention only to the average payoff functions.

In our cyber network security application, mixed Nash strategies are preferred since the existence is guaranteed. In addition, the stochastic property of mixed Nash strategy is compatible to the Markov (stochastic) game model. Playing a mixed strategy can also keep your opponent off balance. The worst case payoff of a mixed strategy may be better than the worst case payoff of a pure strategy.

In our proposed approach, the solution to the Markov game is obtained via a *K* time-step look-ahead approach, in which we only optimize the solution in the *K* time-step horizon. *K* usually takes 2, 3, 4, or 5. The suboptimal technique is used successfully for reasoning in games such as chess, backgammon and monopoly. For our case, the objective of each team at time *k* is to find a serial of actions or COA to maximize the following team level payoffs, respectively,

$$J_k^B(u_k^B,u_k^R,u_k^W,u_{k+1}^B,u_{k+1}^R,u_{k+1}^W,\ldots,u_{k+K}^B,u_{k+K}^R,u_{k+K}^W)=\sum_{i=k}^{k+K}V^B(\tilde{s}^B(i),u_i^B;i) \quad (10)$$

$$J_k^R(u_k^B,u_k^R,u_k^W,u_{k+1}^B,u_{k+1}^R,u_{k+1}^W,\ldots,u_{k+K}^B,u_{k+K}^R,u_{k+K}^W)=\sum_{i=k}^{k+K}V^R(\tilde{s}^R(i),u_i^R;i) \quad (11)$$

$$J_k^W(u_k^B,u_k^R,u_k^W,u_{k+1}^B,u_{k+1}^R,u_{k+1}^W,\ldots,u_{k+K}^B,u_{k+K}^R,u_{k+K}^W)=\sum_{i=k}^{k+K}V^W(\tilde{s}^W(i),u_i^W;i) \quad (12)$$

Remark 5: The *K*-step look-ahead (or moving window) approach well fits the situations in which multi-step cyber network attacks occurs since we evaluate the performance of each team based on the sum of payoffs during a period of *K*-time steps.

3. Simulations and Experiments

To evaluate our game theoretic approach for cyber attack prediction and mitigation, we have constructed a Cyber Game Simulation Platform (CGSP) based on an open-source network experiment specification and visualization tool kit (ESVT). [ESVT] Through this event-based, interactive and visual simulation environment, various attack strategies (single stage or multi-staged) and scenarios can be easily played out and the effect of game theoretic attack prediction and mitigation can be visually and quantitatively evaluated. Fig.2 is a snapshot of the CGSP environment.

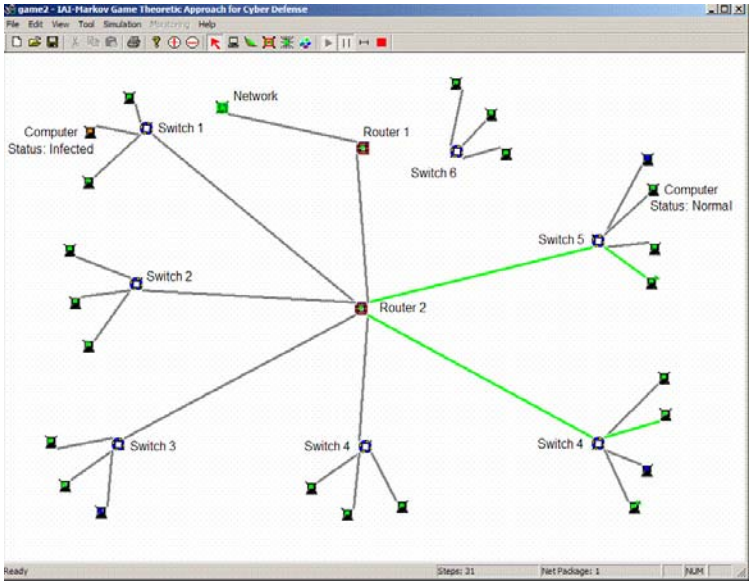


Fig. 2 Cyber Game Simulation Platform (CGSP)

The implemented network components in this platform includes Computer (host), Switch, OSPF Router or Firewall, Link (connection), and (Sub) Network (Simulated by a node).

Besides the ordinary network properties such as processing capacity, bandwidth, and delay etc., CGSP components can be assigned a number of network attack containment or traffic mitigation properties to act as various defense roles, including smart IDS (intrusion detection systems), incoming traffic block, and outgoing traffic block. Additionally and more importantly, these defense roles or network defense properties can be deployed and re-deployed on the fly during a game simulation run-time based on the local intelligence and orders from higher-level command centers.

The color of a link represents the traffic volume on that link (in KBps and in Mbps).

- Light Gray: less than 1 percent of bandwidth
- Green: more than 1 percent of bandwidth
- Yellow: between green and red
- Red: more than 30 percent of bandwidth

The color of a host indicates the host status.

- Red: Infected node.
- Green: Vulnerable node but not infected
- Gray: Non-vulnerable node

Some features of the CGSP include,

- An *integrated environment* to plan and specify interactive network simulation experiments. At the first step, it can be used to draw the network topology and

specify component properties such as susceptibility, server, or non-server, etc. Users can also change the properties of a group of components or all components by invoking the global component and script property configuration window. The topology builder is designed to be scalable and can support large topologies with thousands of components. There is no hard limit on the size of the virtual canvas and the display can be smoothly zoomed in and zoomed out to accommodate editing operation on a large topology.

- *Network protocol neutral*: Network packets and their communication are simulated by high-level event objects and their movement across various components. Specific network protocol details are ignored. We ignore many such technological details so we can focus on attack scenario construction and defense strategies. Preliminary emulation experiments have shown that such network protocol neutral simulation yields a relatively high fidelity.
- *Event driven simulation*. It means to represent and organize network dynamics by events in a network environment and trace all the events. A running event may trigger a new event to be generated. So every step of simulation is to let all the events to be finished if they can finish. Event driven is complemented by object driven since some host will generate new events even when there is no triggering event on the host (For example, during a worm break or a infected host participating in a DoS attack). We define a step of network simulation, which means a non-interruptible time period of the simulation.
- "What you see is what is happening" style *visualization* based simulation. Visualization shows clear advantages in helping network and security researchers understand and make sense of the network dynamics from their experimental results and the CGSP environment is built on this principle. The GUI updates network component and their security status every second and component properties can be inspected and modified interactively during the simulation. Simulation can also be suspended, resumed, and adjusted with respect to running speed.
- Multiple entries for *user intervention*. Experimenters can inject various attack scenarios or defense actions in advance by using the "Timed Event" feature. During the simulation run-time, experimenters can also modify component properties or insert diagnostic or experimental events into the simulation through the graphical user interface. In addition, with the advancements in real-time assessment, user action and cognition can utilize Level 5 fusion (user refinement) [15] to refine high-level understanding of events, detect conflicts, and prioritize nodes for additional details of possible intrusions, attacks, and malicious cyber behavior.
- For router simulation, if we use Dijkstra's Algorithm, then we have to generate a table for every router. Dijkstra's single-source shortest-path algorithm computes all shortest paths from a single vertex. But the storage of such table in every node wastes valuable computer resources. Another algorithm is called Floyd's all-pairs shortest-path algorithm, or the Floyd-Warshall All-Pairs-Shortest-Path algorithm.

It solves all the shortest paths in the same step. We use this algorithm to get the "shortest path" .

In our simulation platform, network attacks and defenses are simulated in CGSP by events. Live network packets and other communications are represented and simulated by the main network event queue. Users or software agents can inject packets or network events through the timed event (M/M/1) queue. Security alerts or logs are generated and stored in the security log queue.

There are a number of cyber attacks that are included in the CGSP implementation: Port scan, Buffer attack (to gain control), Data bomb or Email bomb from and to a single host, Distributed Denial of service from multiple hosts, Worm attack, and Root right hack (confidentiality loss). [Note: Both buffer attack victims and worm infectives will join the distributed denial of service when they receive the DDOS command.]

The arsenal of network defense team includes: Smart IDS (Accuracy and false positive adjustable), Directional traffic block (outgoing or incoming), Host Shutdown, Host Reset (shutdown and restart). [Note: Both SHUTDOWN and RESET will clear the infection status on the host.]

The following level one security logs are generated: Port Scan log, Buffer attack log, Hacked host log, Worm log, Data bomb log, and DoS log.

We simulated three typical scenarios. In the first scenario as shown in Fig. 3, there are 7 computers, 3 routers, 2 switches, and 1 normal outside network.

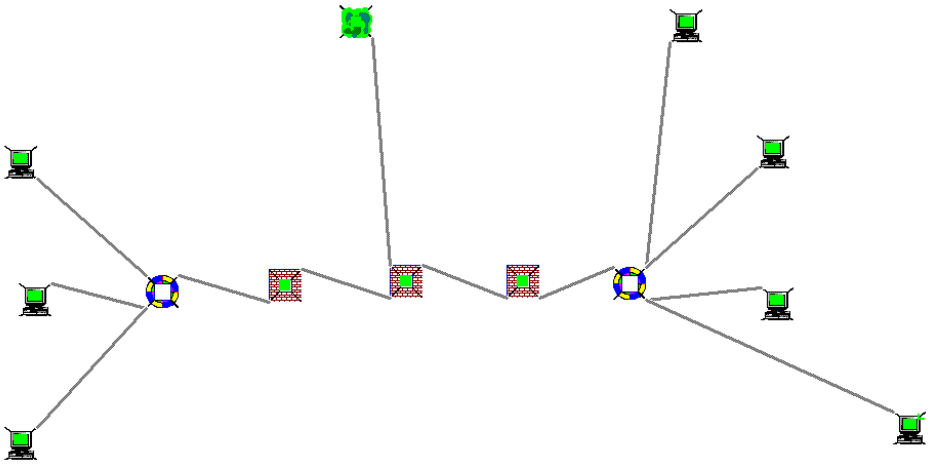


Fig. 3 Scenario 1

Since the network defense side can reset the computers anytime, we can see from the simulation (screen captured movie file scenario1.avi – available upon request) that no servers or target computers are infected or hacked.

In a more complicated scenario 2 as shown in Fig. 2, there are 23 computers, 2 routers, 7 switches, and 1 network. In this scenario, we disable the operation of resetting infected or hacked computers in the action space of cyber network defense side. We can see from Fig. 4 and Fig. 5 that a target computer (web server) is infected or hacked. Then the computer (web server) will be used by attacking force to infect other more important target computers such as file servers or email servers. This two-step attacking scheme is

based on two facts: 1) a public web server is easy to attack and 2) an infected internal computer (web server in this case) is more efficient and stealthy than an external computer to attack well protected computers such as data servers or email servers.

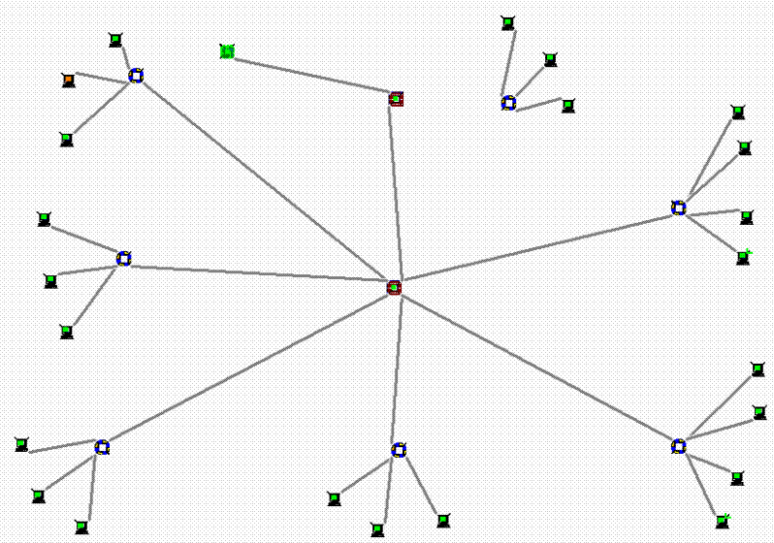


Fig. 4: a public web server is infected or hacked

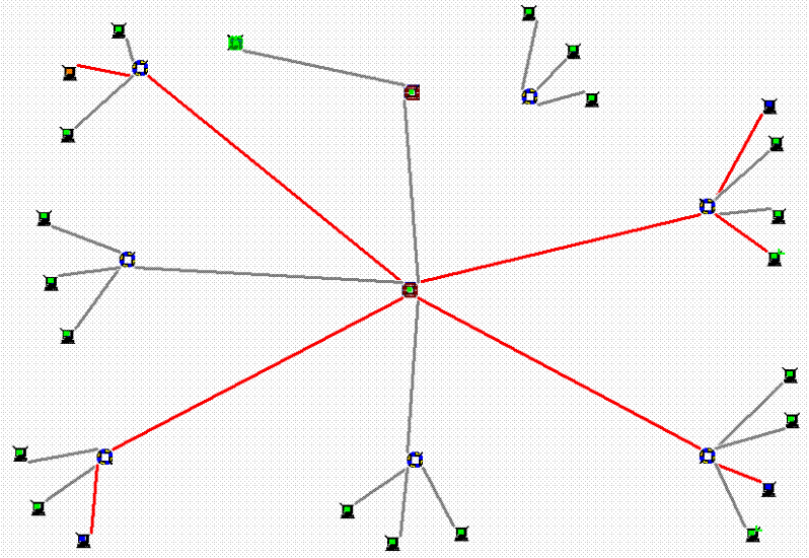


Fig. 5 Three more important data servers are attacked by the infected web server

To test the scalability of our approach, we also simulated a relatively complicated case in the third scenario (Fig. 6), in which 269 computers, 10 routers, and 18 switches are included.

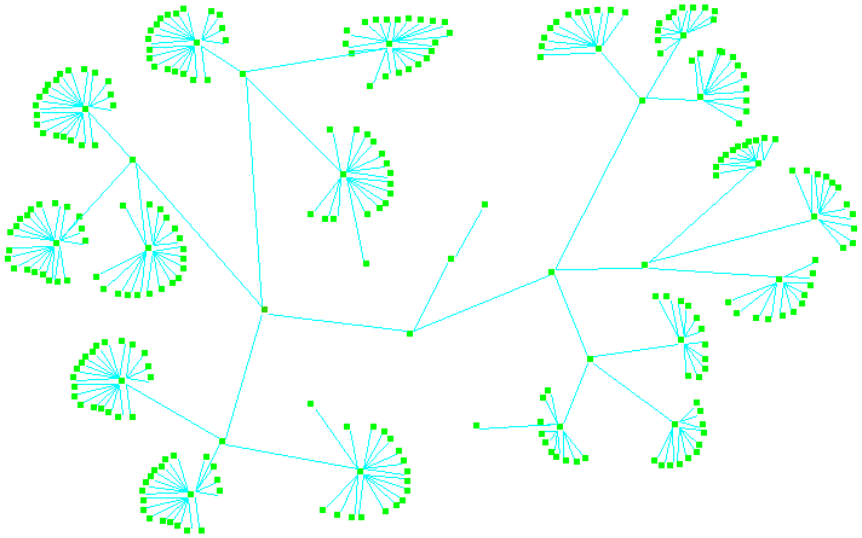


Fig. 6: A complicated network defense scenario with 269 computers

From the simulation (screen captured movie file scenario1.avi – available upon request), we can see that the simulation is slower than the previous two scenarios due to the increased computing work. Fortunately, the intelligent interactions between two sides are well simulated and demonstrated based on our Markov game model.

4. Conclusions

We implemented high level information-fusion/data-mining based situation awareness and adversary intent inference in a cyber attack and network defense scenario. The network security system was evaluated and protected from a perspective of data fusion and adaptive control. The goal of our approach was to examine the estimation of network states and projection of attack activities (similar to ECOA in the warfare scenario). We used Markov game theory's ability to "step ahead" to infer possible adversary attack patterns. Extensive simulations were performed to verify and illustrate the benefits of this model. The performance of our algorithm was very promising. Game theoretic tools have a potential for threat prediction that takes real uncertainties in Red plans and deception possibilities into consideration.

Acknowledgements

This work was supported by the Small Business Innovation Research (SBIR) under Contract N00014-06-M-0237 issued by the Office of Naval Research (ONR). The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the SBIR or ONR.

References

[1] D. Shen, G. Chen, J. B. Cruz, Jr., et al., "Game Theoretic Approach to Threat Intent Prediction," in *Proceedings of CCRTS 2006: the Command and Control Research and Technology Symposium*, San Diego, July, 2006.

[2] Salerno, John J., Michael Hinman, and Douglas Boulware, "A Situation Awareness Model Applied To Multiple Domains", In *Proc of the Defense and Security Conference*, Orlando, FL, March 2005.

[3] Tadda, George, John Salerno, Douglas Boulware, Michael Hinman and Samuel Gorton, "Realizing Situation Awareness within a Cyber Environment", In *Multisensor, Multisource Information Fusion: Architectures, Algorithms, and Applications 2006*, edited by Belur V. Dasarathy, Proceedings of SPIE Vol. 6242 (SPIE, Bellingham, WA, 2006) 624204.

[4] M. Sudit, A. Stotz, and M. Holender, "Situational awareness of a coordinated cyber attack," in *Proceedings of SPIE, Defense and Security Symposium*, March 2005, pp. 114–129.

[5] M. Sudit, A. Stotz, M. Holender, W. Tagliaferri, and K. Canarelli, "Meaasuring situation awareness and resolving inherent high-level fusion obstacles," in *Proceedings of SPIE, Defense and Security Symposium*, vol. 6242, April 2006.

[6] J. Holsopple, S. J. Yang, and M. Sudit, "Tandi: Threat assessment for networked data and information," in *Proceedings of SPIE, Defense and Security Symposium*, vol. 6242, April 2006.

[7] M. G. Ceruti, A. Ashenfelter, R. Brooks, G. Chen, S. Das, G. Raven, M. Sudit, E. Wright, "Pedigree Information for Enhanced Situation and Treat Assessment", the 9th *International Conference on Information Fusion*, Florence, Italy, July 2006.

[8] Jose Cruz, Genshe Chen, Denis Garagic, Xiaohuan Tan, Dongxu Li, Dan Shen, Mo Wei, Xu Wang, "Team Dynamics and Tactics for Mission Planning," *Proceedings, IEEE Conference on Decision and Control*, December 2003.

[9] M. Wei, G. Chen, J. B. Cruz, C. Kwan, and M. Kruger, "Game theoretic modeling and control of military air operations with civilian players," *Proceedings, 2006 AIAA Guidance, Navigation, and Control Conference*, Keystone, Colorado, Aug. 21-24, 2006.

[10] John Nash, "Noncooperative games", *Annals of Mathematics*, vol. 54, pp. 286-295, 1951.

[11] Ertoz, L., Eilertson, E., Lazarevic, A., Tan, P., Srivastava, J., Kumar, V., Dokas, P., "The MINDS - Minnesota Intrusion Detection System,-Next Generation Data Mining", MIT Press, 2004".

[12] L. S. Shapley, "Stochastic games," in P*roceedings of the National Academy of Sciences of the United States of America*, vol. 39, pp. 1095-1100, 1953.

[13] R. Aumann, "Rationality and Bounded Rationality", *Games and Economic Behavior*, vol. 21, pp. 2-14, 1997.

[14] T. R. Gruber, "Toward Principles for the Design of Ontologies Used for Knowledge Sharing", Int. *Journal of Human-Computer Studies*, vol. 43, pp.907-928, 1995.

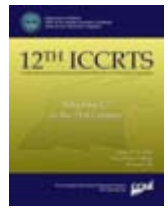
[15] E. Blasch and S. Plano, "DFIG Level 5(User Refinement) issues supporting Situational Awareness Reasoning," Int. *Society of Information Fusion Conference – Fusion05*, 2005.

Game Theoretic Solutions to Cyber Attack and Network Defense Problems

12th ICCRTS

"Adapting C2 to the 21st Century"

Newport, Rhode Island, June 19-21, 2007



Twelfth International Command and Control Research and Technology Symposium

Intelligent Automation, Inc
Dan Shen, Genshe Chen

Cruz & Associates
J. B. Cruz, Jr.

AFRL/SNAA
Erik Blasch

The Office of Naval Research
Martin Kruger

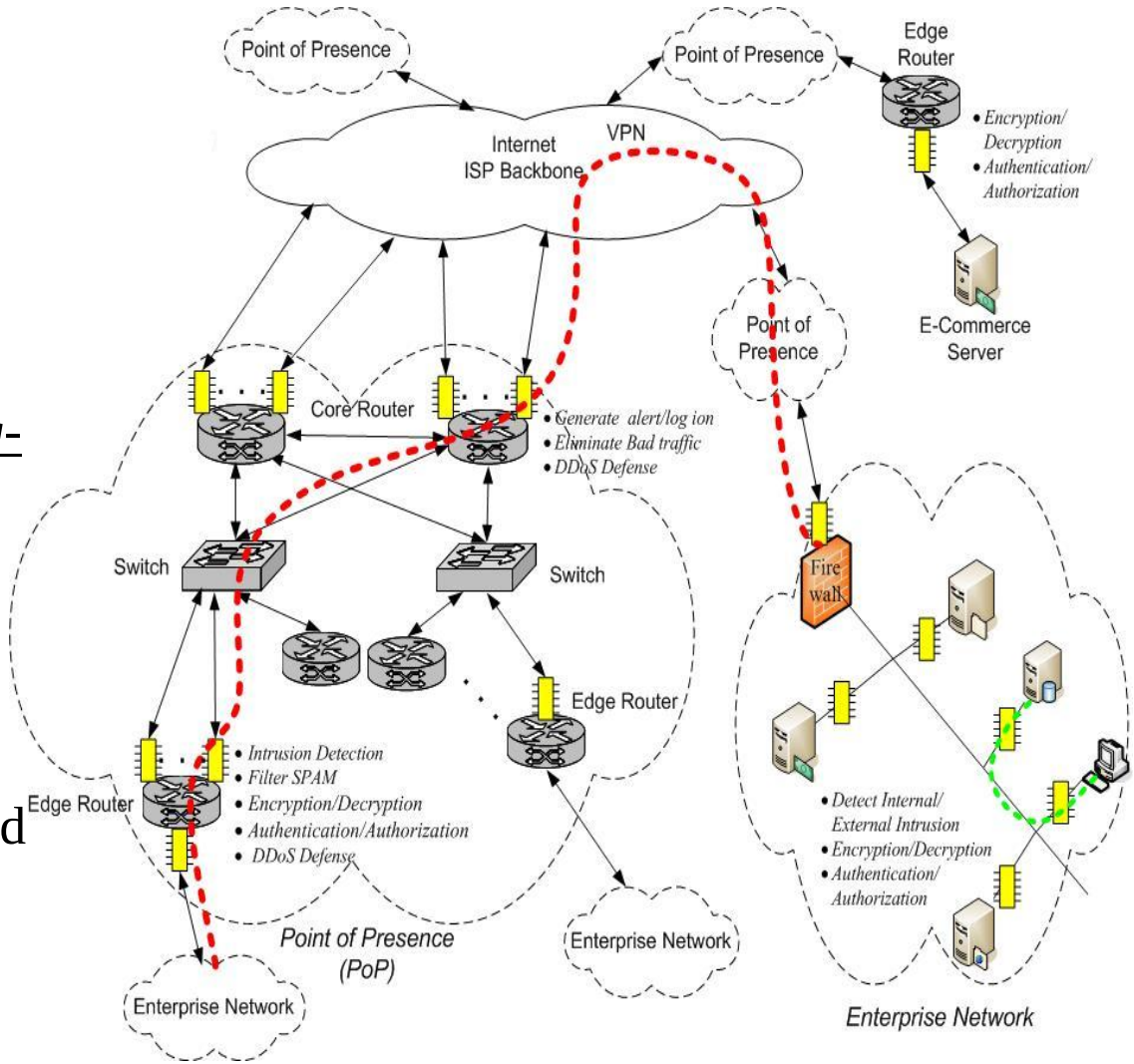
Outline

- Introduction
- Overall Framework
- Markov Game model for Cyber Network Defense
- Simulations and Experiments
- Conclusions

Introduction to the Problem

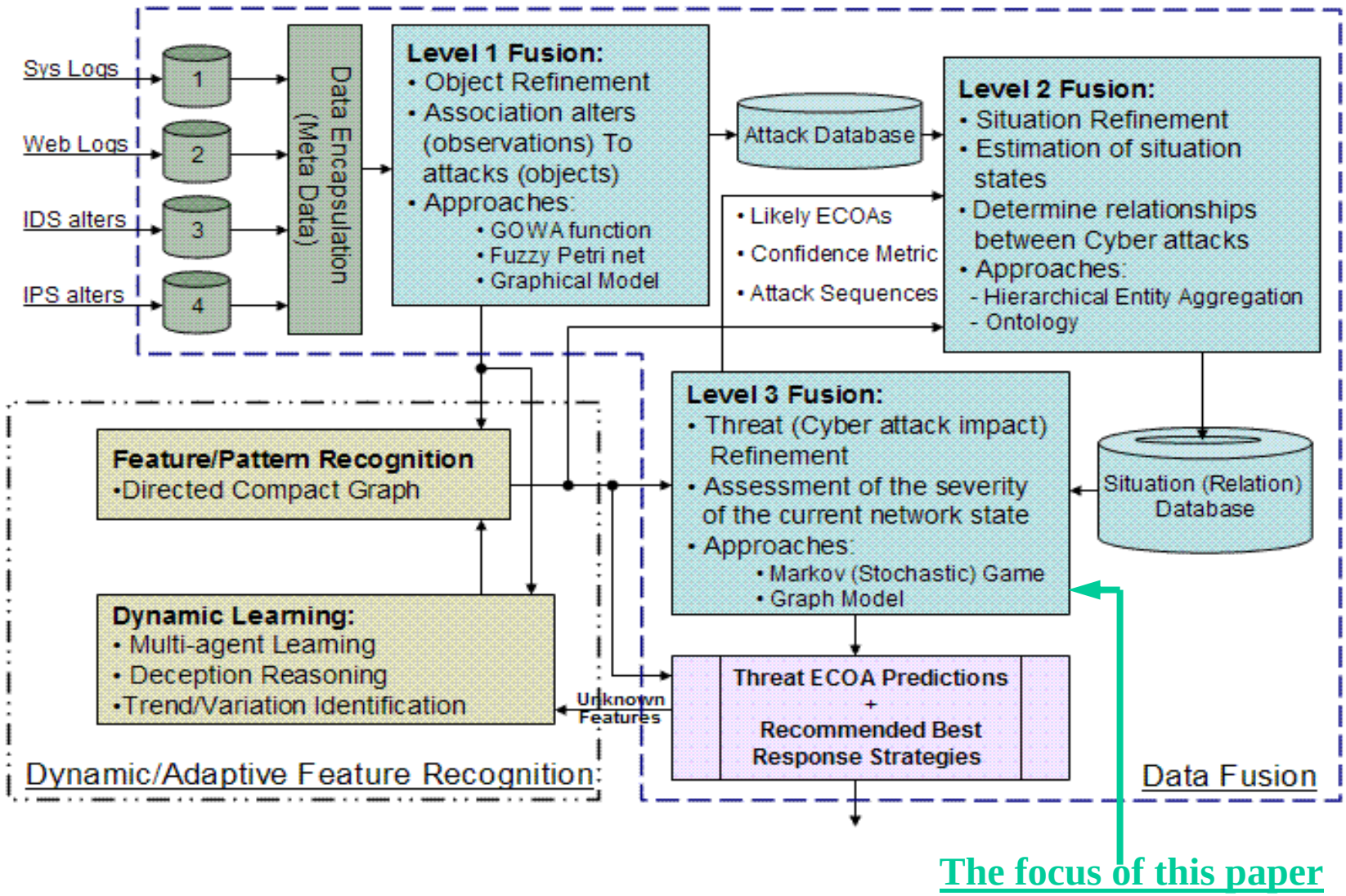
Intelligent Automation, Inc.

- The cyberspace security requires next-generation network management and intrusion detection systems.
- These systems should combine both *short-term sensor information* and *long-term knowledge databases.* to provide decision-support and cyberspace command and control.
- We propose an information fusion and data mining based decision and control framework to detect and predict the multistage stealthy cyber attacks.



System Architecture

Intelligent Automation, Inc.



Key Components

- Similar to the battle-space architecture, our cyberspace security system has two fully coupled major parts:
  - Data fusion module (to refine primitive awareness and assessment; to identify new cyber attacks);
  - Dynamic/adaptive feature recognition module (to generate primitive estimations; to learn new identified new or unknown cyber attacks).
- Various logs and Intrusion Detection Sensors (IDS) alerts are fed into the L1 data fusion components.
- The fused objects and related pedigree information are used by a feature/pattern recognition module to generate primitive prediction of intents of cyber attackers.
- High-level (L2 and L3) data fusion based on Markov game model is proposed to refine the primitive prediction
- The captured unknown/new cyber attack patterns will be associated to related L1 results in dynamic learning block,

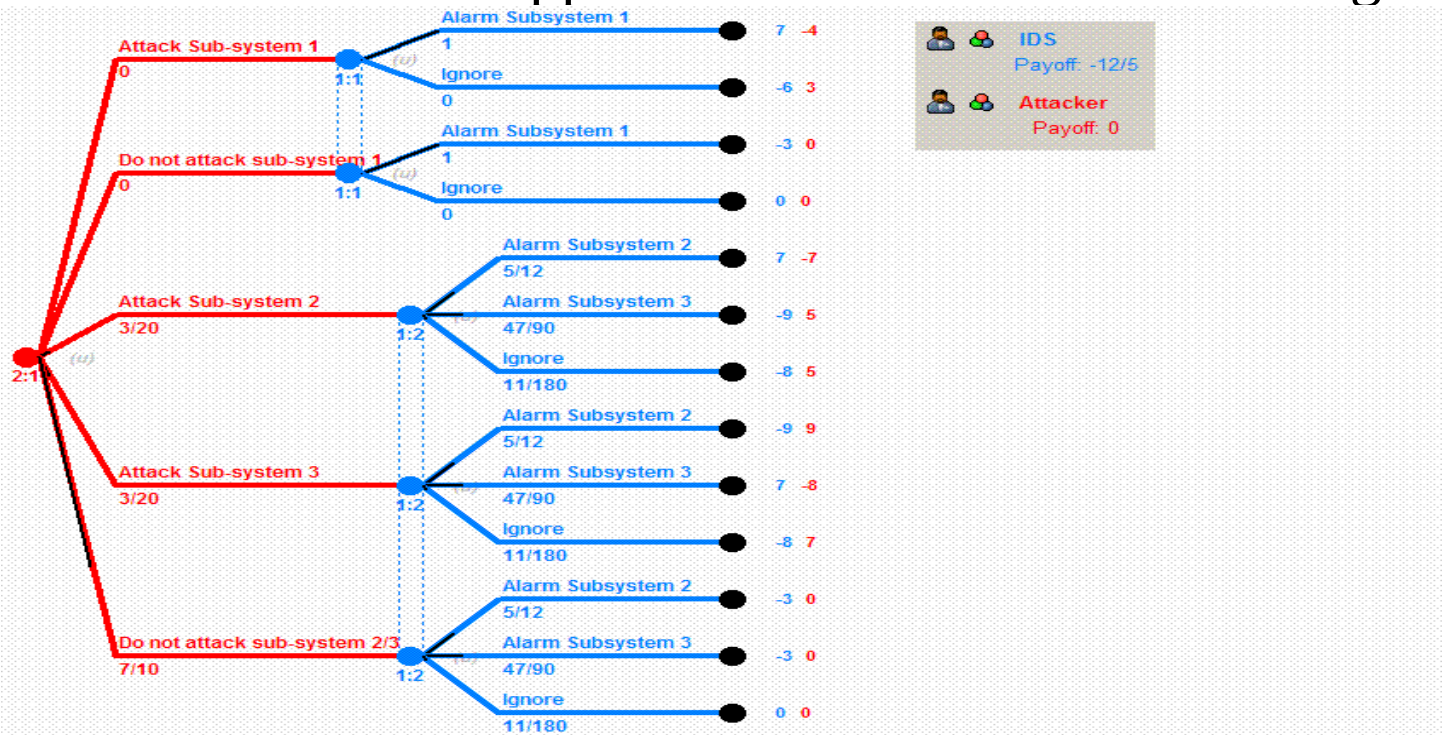
Key Features

- Recognition/Refinement/Learning Structure --- Data mining
- A Decentralized multiplayer non-zero sum Markov Game Model
  - Markov (Stochastic) game model is used to estimate the belief of each possible Enemy Course of Action (ECOA).
  - The actions of white objects are modeled as the *third player* in the non-zero sum Markov game framework.
- A Hierarchical Entity Aggregation
  - Lower level entity (node) aggregation --- clique-based clustering protocol and Fair and Secure Clustering Scheme (FSCS) clustering protocol
  - High level entity (node) aggregation --- a collection of entities collaborating to achieve the *same tactical goal.*
- Ontology
- EWMA (Exponentially Weighted Moving Average)

Game Theoretic Approaches -- Review

Intelligent Automation, Inc.

- Current game theoretic approaches[1-2] for cyber network intrusion detection and decision support are based on static matrix games



1: Attack Sub-system 1	1: Do not attack sub-system 1	1: Attack Sub-system 2	1: Attack Sub-system 3	1: Do not attack sub-system 2/3
0	0	$\frac{3}{20}$	$\frac{3}{20}$	$\frac{7}{10}$

1: Alarm Subsystem 1	1: Ignore	2: Alarm Subsystem 2	2: Alarm Subsystem 3	2: Ignore
1	0	$\frac{5}{12}$	$\frac{47}{90}$	$\frac{11}{180}$

[1] T. Alpcan and T. Basar, "A game theoretic application to decision and analysis in Network Intrusion Detection", 42nd IEEE CDC 2003, pp. 2595-2600, Maui, Hawaii, USA

[2] A. Agah, S. K. Das and K. Basu, "A non-cooperative game approach for intrusion detection in sensor networks", Vehicular Technology Conference, 2004. VTC2004-Fall. pp. 2902 – 2906

A Decentralized Markov Game Model

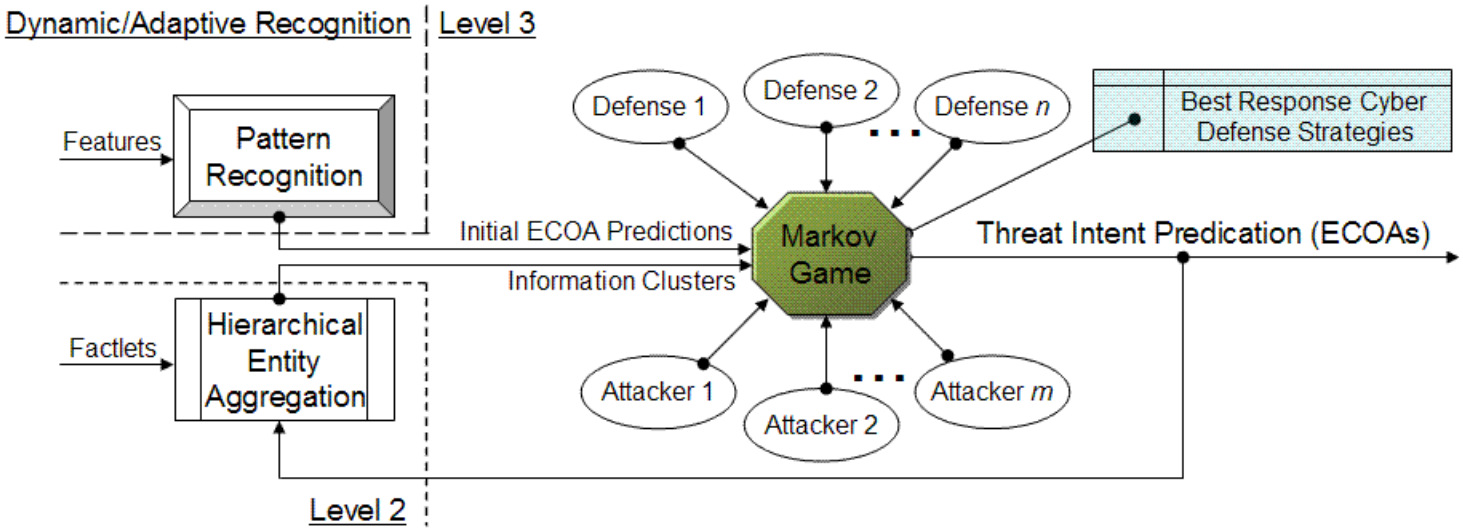
- It is not difficult to see that these matrix game models lack the sophistication to study multi-players with relatively large actions spaces, and large planning horizons.
- For the cyber decision support and attacker intent inference problem, we will revise the dynamic Markov game model[1] used for battle-space and focus on the cyber attack domain properties.
- Our approach has several features:
  - *Decentralized*. Each cluster or team of IDSs makes decisions mostly based on the local information. We put more autonomies in each group allowing for more flexibilities;
  - *Markov Decision Process* (MDP) can effectively model the uncertainties in the cyber network environment;
  - *Game framework* is an effective and ideal model to capture the nature of network conflicts;
  - *White (neutral) objects* (normal network nodes) are modeled as one of the multi-players so that their possible COA will be estimated and considered by the other players.

[1] G. Chen, D. Shen, J. B. Cruz, C. Kwan, and M. Kruger, "Game theoretic approach to threat prediction and situation awareness," ***Proceedings of 9th International Conference on Information Fusion***, Florence, Italy, 10-13 July, 2006

A Decentralized Markov Game Model

Intelligent Automation, Inc.

- Block Diagram



- In general, a Markov (stochastic) game is specified by
  - (i) a finite set of players
  - (ii) a set of states
  - (iii) for every player, a finite set of available actions
  - (iv) a transition rule
  - (v) a payoff function for each player

Player (decision maker)

- Cyber attackers, network defense system, and normal network users are players of this Markov game model.
- We denote cyber attackers as red team, network defense system (IDSs, Firewalls, Email-Filters, Encryption) as blue team, normal network user as white team.
- The cooperation within same team is also modeled so that the coordinated cyber network attacks can be captures and predicted. (Note the cooperation within a team is actually modeled by lower level cooperative games among team members, see section payoff function for details)

State Space

- All the possible states of involved network nodes consist of the state space. (It is different from the battle space model in which the COAs are system states).
- To determine the optimal IDS (intrusion detection sensor) deployment, we include the defense status for each network node in the state space.
- So for the i^{th} network node, there is a state vector $s_i(k)$ at time k.

$$s^i(k) = (f, p, a)^T$$

where f is the working status of the i^{th} network node, p is the protection status, and a is the status of being attacked.

- The system states are determined by two factors: 1) previous states and 2) the current actions. So the whole system can be model by a first-order Markov decision process.

Action Space

- At every time step, each player chooses targets with associated actions based on its local network information.
- The action control of the i^{th} white player at time k is

$$u_w^i(k) = (t, v)^T$$

where vector t is the network node providing services and v is the service types requested.

- For red team (cyber network attackers), we consider the following types of network-based attacks: Buffer overflow, Semantic URL attack, E-mail Bombing, E-mail spam and Distributed Denial-of-service (DDos).
- For blue team (network defense system), we consider the following defense actions: IDS deployment, Firewall configuration , Email-filter configuration, and Shut down or reset servers

Transition Rule

- For each network node (server or workstation), the state of time $k+1$ is determined by three things:
  - state at time k;
  - control strategies of the three teams
  - the attack/defense efficiency.
- From a perceptive of battle-space control, the counterpart of attack/defense efficiency is the kill probability of weapons.
- For example, if the state of node 1 at time k is [“normal”, “NULL”, “NULL”], one component of red action is “email-bombing node 1”, one component of blue action is “email-filter –configuration-no-block for node 1”, and all white actions are not related to node 1, then the probability distribution of all possible next states of node 1 is:
  - [“normal”, “email-filter-configuration”, “email-bombing”] with probability *0.4*
  - [“slow”, “email-filter-configuration”, “email-bombing”] with probability *0.3*
  - [“crashed”, “email-filter-configuration”, “email-bombing”] with probability *0.3*.

Payoff Functions

- In our proposed decentralized Markov game model, there are two levels of payoff functions for each team (red, blue, or white):
  - Low-level (cooperative within each team)
  - High-level (non-cooperative between teams) payoff functions
  - This hierarchical structure is important to model the coordinated cyber network attacks and specify optimal coordinated network defense strategies and IDS deployment.
- The lower level payoff functions are used by each team (blue, red or white side) to determine the cooperative team actions for each team member based on the available local information.
- The top level payoff functions at time *k* are used to evaluate the overall performance of each team.
- In our approach, the lower lever payoffs are calculated distributedly by each team member and sent back to network administrator via communication networks.

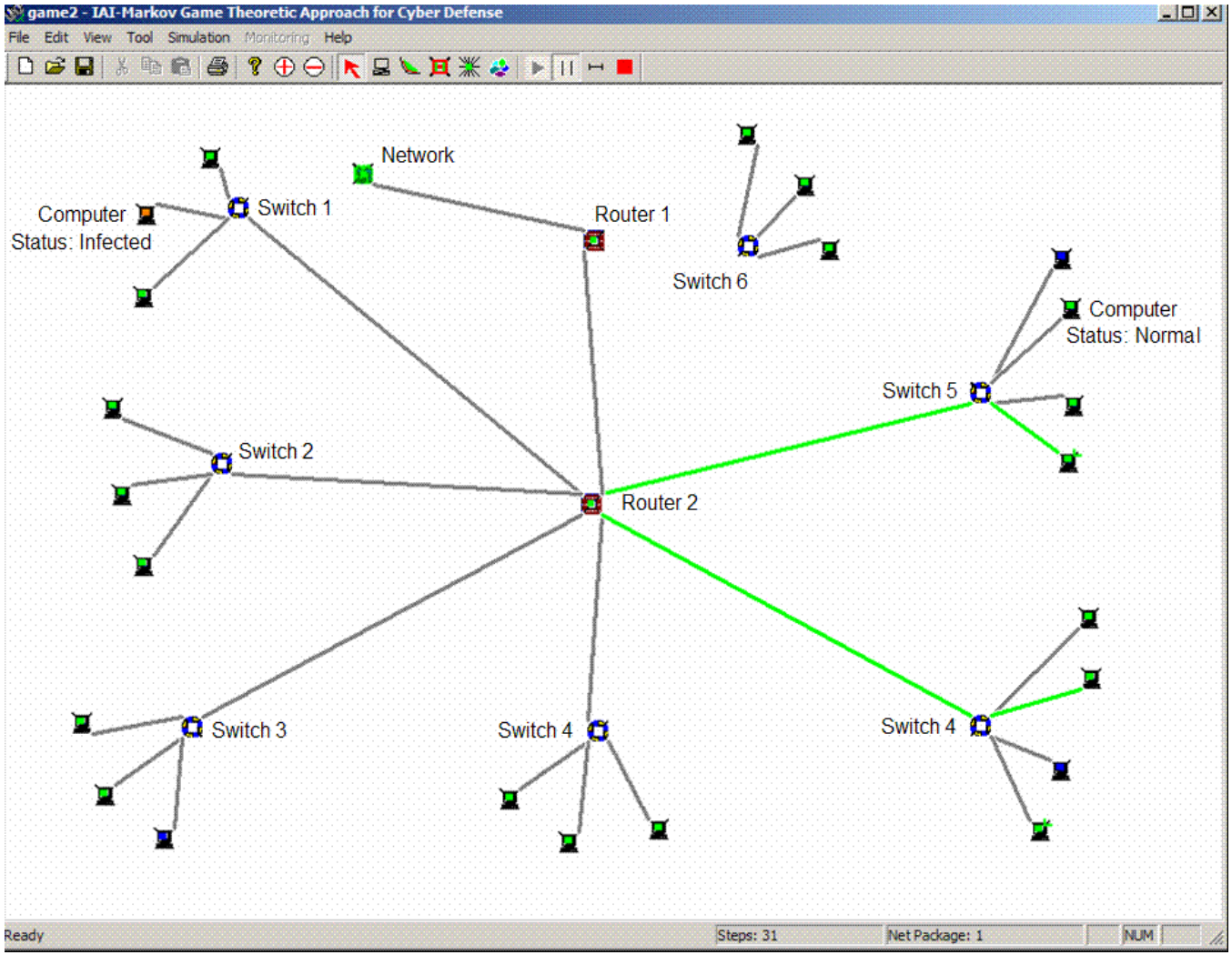
Strategies

- In game theory, the Nash equilibrium is a kind of optimal collective strategy in a game involving two or more players, where no player has anything to gain by changing only his or her own strategy.
- A mixed strategy is used in game theory to describe a strategy comprised of possible actions and an associated probability, which corresponds to how frequently the action is chosen.
- It was proved by Nash that that every finite game has Nash equilibria but not all has a pure strategy Nash equilibrium.
- In our cyber network security application, *mixed Nash strategies* are preferred since
  - the existence is guaranteed
  - the stochastic property of mixed Nash strategy is compatible to the Markov (stochastic) game model
  - Playing a mixed strategy can also keep your opponent off balance. The worst case payoff of a mixed strategy may be better than the worst case payoff of a pure strategy.

Simulations and Experiments

Intelligent Automation, Inc.

- Simulation software - Cyber Game Simulation Platform (CGSP)



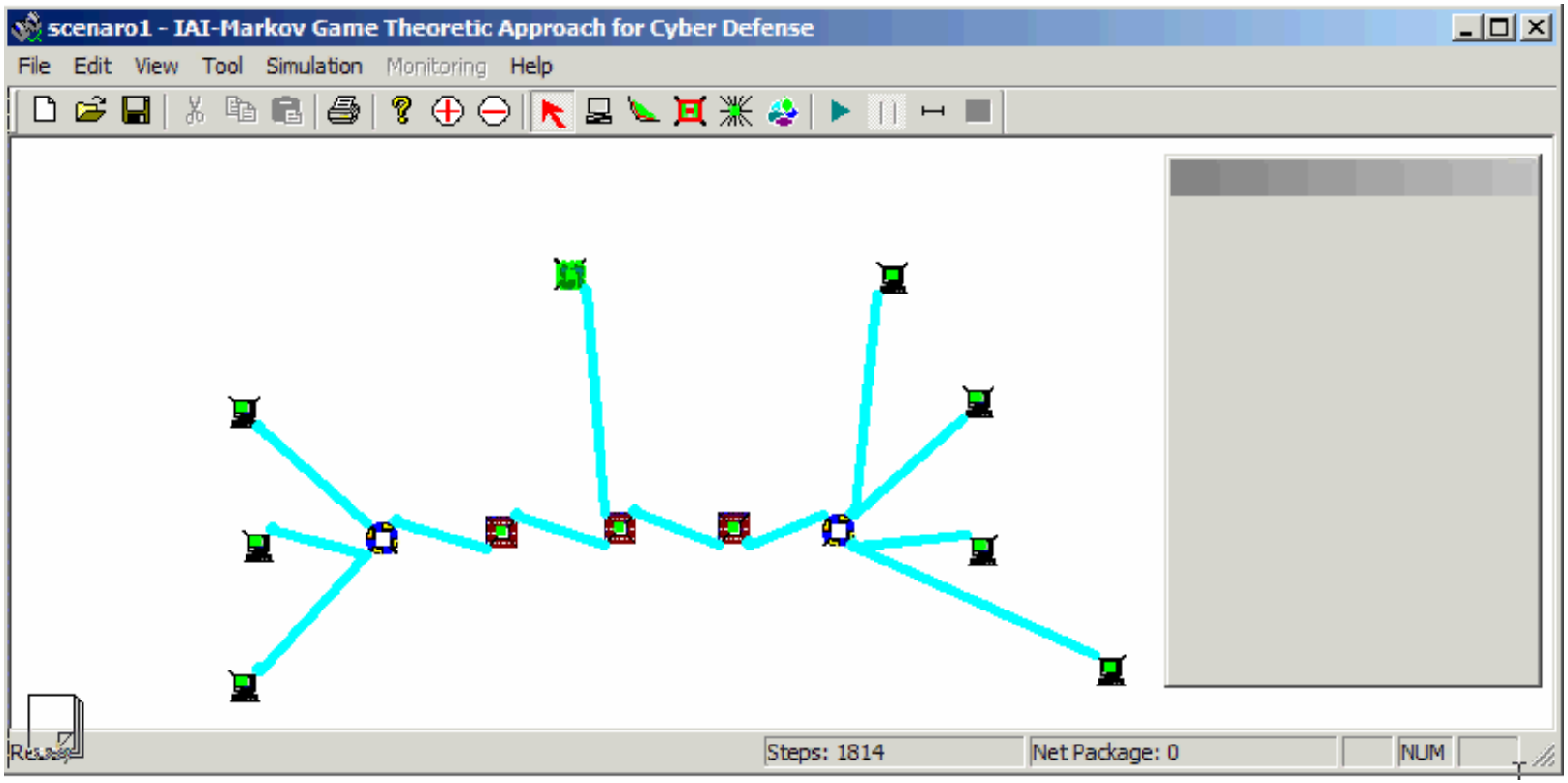
Simulations and Experiments

- Simulation software - Cyber Game Simulation Platform (CGSP)
  - The implemented network components: Computer (host), Switch, Open Shortest Path First (OSPF) Router or Firewall, Link (connection), and (Sub) Network (Simulated by a node).
  - The color of a link represents the traffic volume on that link (in KBps and in Mbps).
    - Light Gray: less than 1 percent of bandwidth
    - Green: more than 1 percent of bandwidth
    - Yellow: between green and red
    - Red: more than 30 percent of bandwidth
  - The color of a host indicates the host status.
    - Red: Infected node.
    - Green: Vulnerable node but not infected
    - Gray: Non-vulnerable node

Scenario 1 – “reset” enabled

Intelligent Automation, Inc.

- There are 7 computers, 3 routers, 2 switches, and 1 normal outside network.

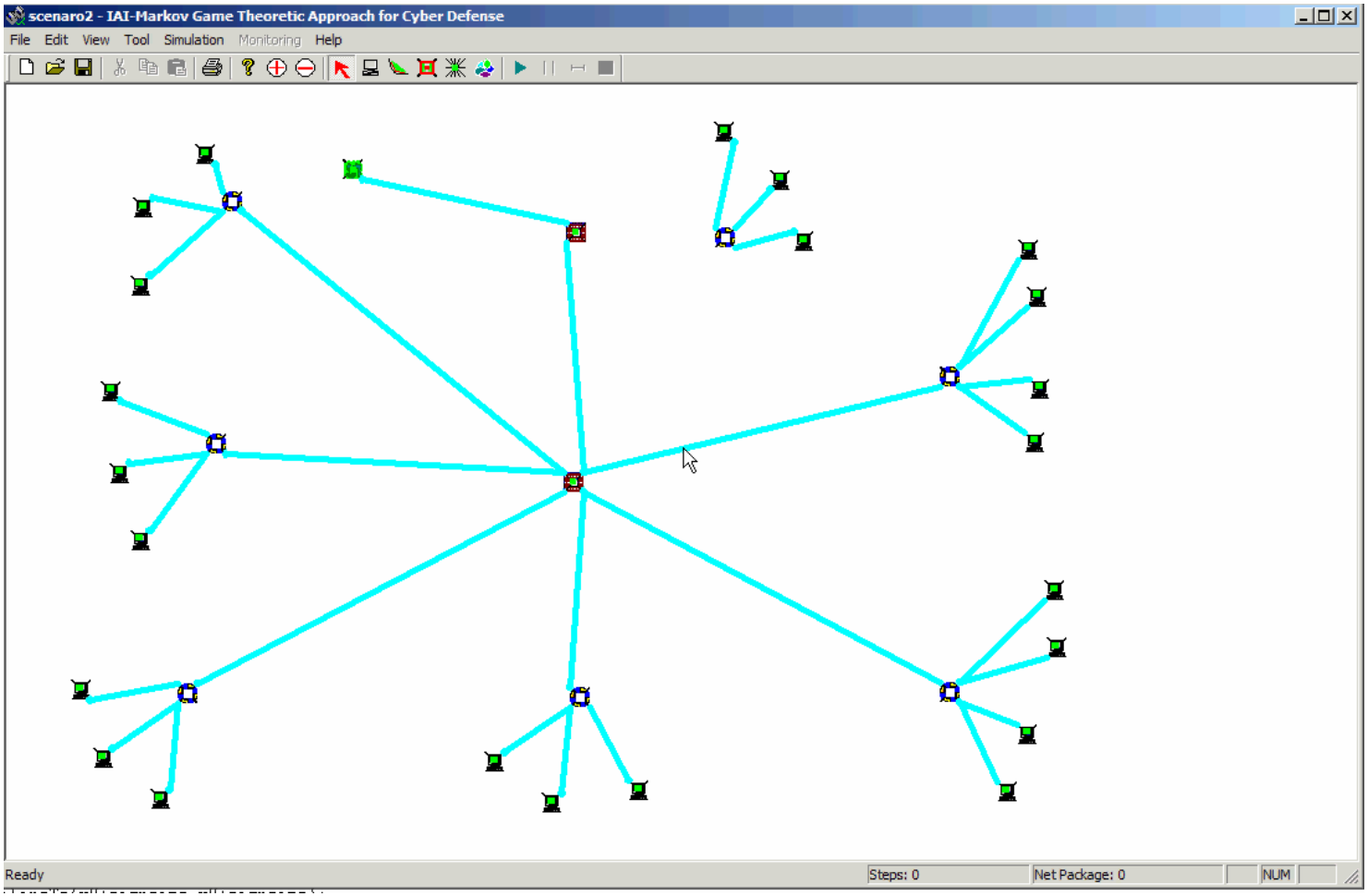


Since the network defense side can reset the computers anytime, we can see from the simulation that no servers or target computers are infected or hacked.

Scenario 2– “reset” disabled

Intelligent Automation, Inc.

- There are 23 computers, 2 routers, 7 switches, and 1 network.

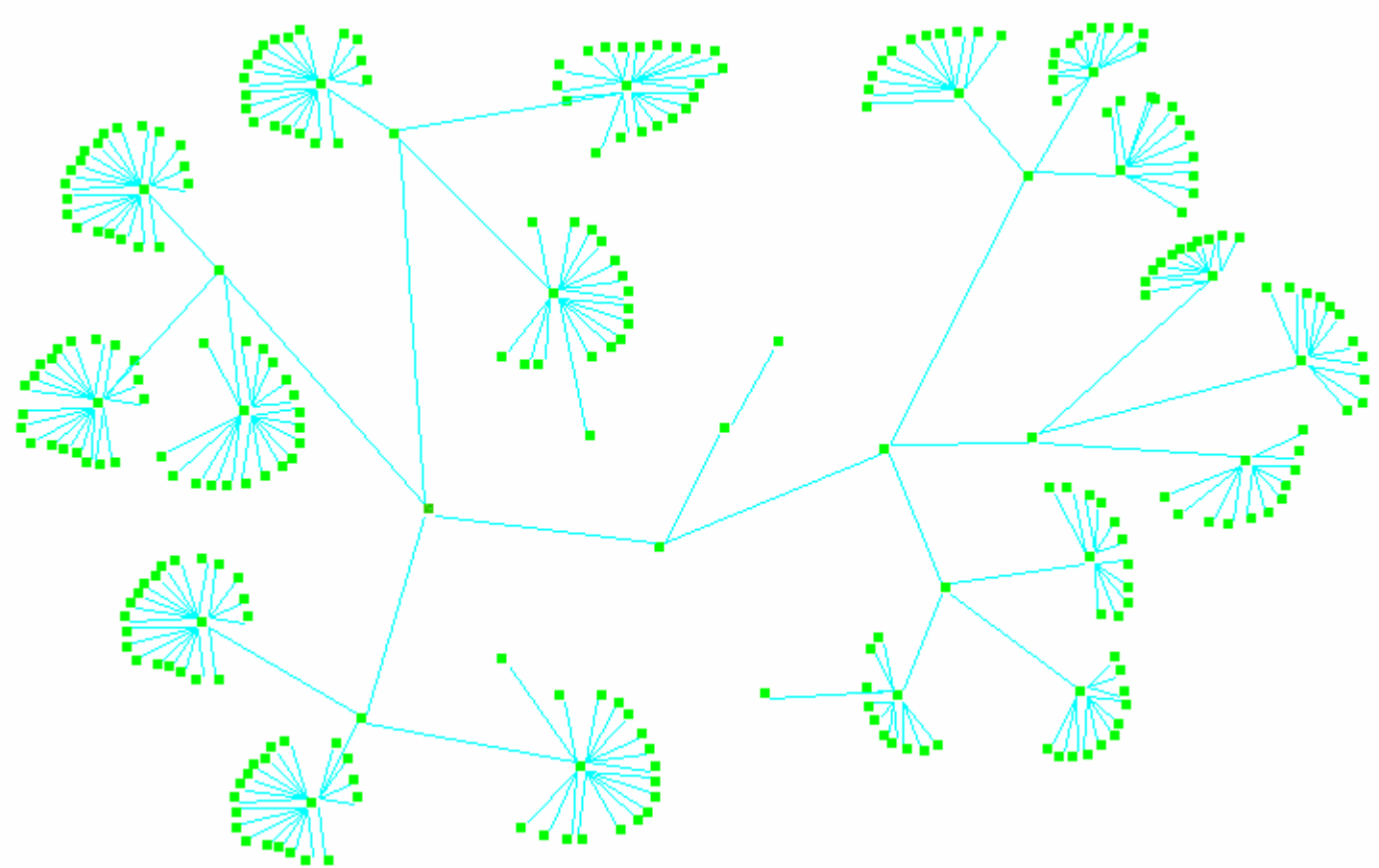


a target computer (web server) is infected or hacked. Then the computer (web server) will be used by attacking force to infect other more important target computers such as file servers or email servers.

Scenario 3– scalability test

Intelligent Automation, Inc.

- There are 269 computers, 10 routers, and 18 switches.



We can see that the simulation is slower than the previous two scenarios due to the increased computing work. Fortunately, the intelligent interactions between two sides are well simulated and demonstrated based on our Markov game model.

Conclusions

- The network security system was evaluated and protected from a perspective of data fusion and adaptive control.
- The goal of our approach was to examine the estimation of network states and projection of attack activities (similar to ECOA in the warfare scenario).
- We used Markov game theory's ability to "step ahead" to infer possible adversary attack patterns.
- Extensive simulations were performed to verify and illustrate the benefits of this model.
- Game theoretic tools have a potential for threat prediction that takes real uncertainties in red plans and deception possibilities into consideration.